UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/743,119	12/22/2003	W. Carey Bunn	END920030045US1	7503

26502 7590 07/06/2011

IBM CORPORATION
IPLAW SHCB/40-3
1701 NORTH STREET
ENDICOTT, NY 13760

EXAMINER	
SCHMIDT, KARL	

ART UNIT	PAPER NUMBER
2439	

NOTIFICATION DATE	DELIVERY MODE
07/06/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

endiplaw@us.ibm.com

Office Action Summary	Application No.	Applicant(s)	
	10/743,119	BUNN ET AL.	
	Examiner	Art Unit	
	KARI SCHMIDT	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 April 2011*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *16 and 21-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *16 and 21-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Notice to Applicant

This communication is in response to the amendment filed on 04/20/2011. Claims 16 and 21-37 are pending in the application. Claim 16 has been amended. Claims 1-15 and 17-20 have been canceled. Claims 21-37 have been newly added.

Response to Arguments

Applicant's arguments with respect to claims 16 and 21-37 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 16, 21, 23-24, 26-27, 29, 30, 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kurtz et al. (US 2003/0217039 A1) in view of Trcka et al. (US 6,453,345 B2) and Subramaniam et al. (US 6,950,936 B2)

Claims 16, 26, and 32

Kurtz discloses a compute program product for access security of a network perimeter (see at least, abstract), the computer program product comprising: one or more

computer-readable tangible storage devices and program instructions stored on at least one of the one or more storage devices (see at least, FIG. 1 and [0042]), the program instructions comprising: program instructions to review security of the network perimeter by executing tests to attempt to circumvent security controls of the network perimeter (see at least, abstract and [0011]: the examiner notes ...a multiple tier port scanning method... a vulnerability assessment [0012]); program instructions to review security of an application that transfers data across the network perimeter by analyzing message flows and protocol used by the application (see at least, [0028]: the examiner notes ...first and second data packets... compliant with a protocol supported by the network... fingerprint and [0088]); program instructions to review vulnerability of a gateway computer at the network perimeter from applications outside of the network perimeter by scanning ports on the gateway computer to determine whether unauthorized services from the applications outside the network perimeter are available within the network perimeter via the gateway computer (see at least, FIG. 1: Central Intranet Hub and/or Hosts and [0011]: a multiple-tier port scanning method and [0449]), and determining and executing penetration tests on the gateway computer to attempt to exploit a vulnerability of the gateway computer as revealed by the scanning of ports on the gateway computer (and [0011]: the examiner notes ...a multiple tier port scanning method... a vulnerability assessment [0012]); program instructions to generate a report of security of the network perimeter based upon results generated by the program instructions to review security of the network perimeter, the program instructions to review security of applications that transfer data across the network perimeter, and the

program instructions to review vulnerability of the gateway computer at the network perimeter (see at least, abstract).

Kurtz fails to disclose program instructions to review security of a firewall at the network perimeter by analyzing message flow rules of the firewall; program instructions to review security of an authentication computer from attack, the authentication computer residing within the network perimeter and authenticating users outside of the network perimeter that requests access to an application within the network perimeter; program instructions to generate a report of security of the network perimeter based upon results generated by the program instructions to review security of the firewall and the program instructions to review security of the authentication computer.

Trcka discloses program instructions to review security of a firewall at the network perimeter by analyzing message flow rules of the firewall (see at least, col. 20, lines 54-56: the examiner notes replaying of previously recorded intrusion sequence is interpreted to be analyzing message flow rules of the firewall) and program instructions to generate a report of security of the network perimeter based upon results generated the program instructions to review security of the firewall (see at least, col. 10, lines 17-20).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Kurtz to include program instructions to review security of a firewall at the network perimeter by analyzing message flow rules of the firewall and program instructions to generate a report of security of the network perimeter based upon results generated the program instructions to review security of

the firewall as taught by Trcka. One of ordinary skill in the art would have been motivated to combine the teachings in order to detect and protect against security breaches (both internal and external) (see at least, Trcka: col. 1, lines 10-15).

Kurtz in view of Trcka fail to disclose program instructions to review security of an authentication computer from attack, the authentication computer residing within the network perimeter and authenticating users outside of the network perimeter that requests access to an application within the network perimeter; program instructions to generate a report of security of the network perimeter based upon results generated by the program instructions to review security of the authentication computer.

Subramaniam discloses an authentication computer residing within the network perimeter and authenticating users outside of the network perimeter that requests access to an application within the network perimeter (see at least, abstract and FIG. 1: the examiner notes border server).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Kurtz in view of Trcka to include an authentication computer residing within the network perimeter and authenticating users outside of the network perimeter that requests access to an application within the network perimeter as taught by Subramaniam to thereby combine prior art elements according to known methods to yield predictable results and/or simple substitution of one known element for another to obtain predictable results (i.e., placing Subramanian's Border Server in the target network of Kurtz and performing similar testing/reporting as taught by Kurtz) . One of ordinary skill in the art would have been motivated to

combine the teachings in order to provide convenient, efficient, and secure access to data stored on a sever located within a secure network (see at least, Subramaniam: col. 3, lines 9-14).

Claims 21, 27 and 33

Kurtz fails to disclose wherein the program instructions to review security of a firewall including program instructions to assess protection by the firewall against probing into the network perimeter apart from vulnerability to subsequent related attack via the firewall, based in part on the message flow rules of the firewall.

Trcka discloses wherein the program instructions to review security of a firewall including program instructions to assess protection by the firewall against probing into the network perimeter apart from vulnerability to subsequent related attack via the firewall, based in part on the message flow rules of the firewall (see at least, col. 20, lines 54-56: the examiner notes replaying of previously recorded intrusion sequence is interpreted to be analyzing message flow rules of the firewall).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Kurtz to include wherein the program instructions to review security of a firewall including program instructions to assess protection by the firewall against probing into the network perimeter apart from vulnerability to subsequent related attack via the firewall, based in part on the message flow rules of the firewall as taught by Trcka. One of ordinary skill in the art would have

been motivated to combine the teachings in order to detect and protect against security breaches (both internal and external) (see at least, Trcka: col. 1, lines 10-15).

Claims 23, 29, and 35

Kurtz discloses wherein the application that transfers data across the network perimeter is installed in a computer system, and further comprising program instructions, stored on at least one of the one or more storage devices, to scan ports of the computer system to determine whether unauthorized services are available within the network perimeter from the computer system, and identify and execute penetration tests on the computer system to attempt to exploit a vulnerability of the computer system as revealed by the scanning of the ports on the computer system (see at least, [0028]: the examiner notes ...first and second data packets... compliant with a protocol supported by the network... fingerprint and [0088]).

Claims 24, 30, and 36

Kurtz further comprising program instructions, stored on at least one of the one or more storage devices, to review security of a server computer within the network perimeter that provides data to an application outside of the perimeter (see at least, abstract, [0012], and [0019]).

Claims 22, 25, 28, 34, and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kurtz et al. (US 2003/0217039 A1) in view of Trcka et al. (US 6,453,345 B2) and Subramaniam et al. (US 6,950,936 B2) as applied to respective claim(s) above, and further in view of Chandrashekhar et al. (US 2003/0212909 A1)

Claims 22, 28 and 34

Kurtz in view of Trcka and Subramaniam fail to disclose further comprising program instructions, stored on at least one of the one or more storage devices, to review security of the application that transfers data across the network perimeter based on a location of data transferred by the application and whether the transferred data is encrypted.

Chandrashekhar discloses further comprising program instructions, stored on at least one of the one or more storage devices, to review security of the application that transfers data across the network perimeter based on a location of data transferred by the application and whether the transferred data is encrypted (see at least, Table 1 and [0023] and [0093]).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Kurtz in view of Trcka and Subramaniam to include further comprising program instructions, stored on at least one of the one or more storage devices, to review security of the application that transfers data across the network perimeter based on a location of data transferred by the application and whether the transferred data is encrypted as taught by Chandrashekhar. One of

ordinary skill in the art would have been motivated to combine the teachings in order to provide a systematic way to analyze the security capabilities of a given network architecture, either for an existing network, a network being modified, or a network being deployed (see at least, Chandrashekhar: [0003]).

Claim 25, 31, and 37

Kurtz in view of Trcka and Subramaniam fail to disclose further comprising program instructions, stored on at least one of the one or more storage devices, to review security of the application that transfers data across the network perimeter based on a location of data transferred by the application and whether the transferred data is encrypted.

Chandrashekhar discloses further comprising program instructions, stored on at least one of the one or more storage devices, to review security of the application that transfers data across the network perimeter based on a location of data transferred by the application and whether the transferred data is encrypted (see at least, Table 1 and [0023] and [0093]).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Kurtz in view of Trcka and Subramaniam to include further comprising program instructions, stored on at least one of the one or more storage devices, to review security of the application that transfers data across the network perimeter based on a location of data transferred by the application and whether the transferred data is encrypted as taught by Chandrashekhar. One of

ordinary skill in the art would have been motivated to combine the teachings in order to provide a systematic way to analyze the security capabilities of a given network architecture, either for an existing network, a network being modified, or a network being deployed (see at least, Chandrashekhar: [0003]).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KARI SCHMIDT whose telephone number is (571)270-1385. The examiner can normally be reached on Monday - Friday: 8:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on 571-272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kari L Schmidt/
Examiner, Art Unit 2439

/Edan Orgad/
Supervisory Patent Examiner, Art Unit 2439